REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendment and the following remarks.

Claims 1-31 are pending in this application. In the Office Action, the Examiner rejected claims 1-5, 8-12, 14, and 29-30 under 35 U.S.C. § 102(b) as being anticipated by U.S. Publication No. 2002/112171 to Ginter et al. ("Ginter"). The Examiner rejected claims 1-5, 8-12, 14, and 29-30 under 35 U.S.C. § 102(b) as being anticipated by U.S. Publication No. 2002/112162 to Cocotis et al. ("Cocotis"). The Examiner rejected claims 1, 2, 5-7, 10-11, 28, 29, and 31 under 35 U.S.C. § 102(b) as being anticipated by PCT Publication No. WO 01/84319 to XTEC.

The Examiner rejected claims 6, 7, 13, and 15-27 under 35 U.S.C. § 103(a) as being unpatentable over Ginter and Cocotis. The Examiner rejected claims 1-11, 14-18, and 29-30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,426,750 to Cooper et al. ("Cooper"), and further in view of U.S. Patent No. 6,170,060 to Mott et al. ("Mott"). The Examiner rejected claims 12-13 and 26-27 under 35 U.S.C. § 103(a) as being unpatentable over Cooper and Mott as applied to claim 1, and further in view of U.S. Publication No. 20030208338 to Challener et al. ("Challener"). The Examiner rejected claims 19-25 under 35 U.S.C. § 103(a) as being unpatentable over Cooper and Mott as applied to claim 1, and further in view of PCT Publication No. WO 00/67143 to Unicate ("Unicate").

Applicants have amended claims 1, 8, 28, 29 and 31 to further distinguish the claimed invention from the prior art of record in this application. Claims 7 and 10 have been amended

for consistency. New claim 32 has been added, and claims 6, 9 and 30 are hereby cancelled without disclaimer or prejudice. For the reasons stated below, Applicant respectfully submits that all claims pending in this application are in condition for allowance.

General Remarks

The present invention, as recited in the pending claims, is very different from the well-known asymmetric private key/public key cryptographic structure that is disclosed, for example, in the Ginter, Cocotis and Cooper references cited by the Examiner. The private key/public key structure requires elaborate key management systems and operations by the issuer of the public and private key pairs. It also requires the distribution of the private keys in a secure manner. The private key is applied *in its entirety* to generate a digital signature or to encrypt data, and the public key is also applied *in its entirety* to verify a digital signature or to decrypt data. The digital signatures are *verified* by the recipient. The parties must have systems and applications at both ends of the system so that the recipient can retrieve the public key to perform the decrypt function. The private key/public key system disclosed in the prior art does not create or derive transaction specific session keys, *i.e.*, it does not use only a part of either the public key or the private key. In a private key/public key system disclosed in the prior art, it is impossible to generate a digital signature or to encrypt data with only a *part* of a private key, and to validate the digital signature or decrypt the data with an (entire) public key. Private and public keys are distributed only once, and therefore are *static* and *non-session specific*. Moreover, the prior art does not disclose any relationship between session specific data and any key corresponding to (dynamic) session keys.

In contrast, the present invention does not use any additional hardware, and identifies the first transaction party in an electronic transaction by a unique identifiable digital signature, which is provided to the second transaction party, so that the second transaction party may store the digital signature. Later, if a problem arises, the first transaction party may be traced and identified by the digital signature that is provided to the second transaction party.

The present invention does not address digital signature verification and does not address encryption per se. Instead, it teaches a method for storing a digital signature that can later be used to identify and trace the first transaction party. *See, e.g.,* page 3, line 17 to page 4, line 5. Thus the present invention solves a completely different problem in a completely different way than does Ginter, Cocotis, or any of the other prior art of record in this application.

Claims 1 and 29 have been amended to specify that the digital signature is generated by gathering session-specific data and hashing the session-specific data to obtain reference numbers referring to positions in the authentication data. These limitations were (and still are) recited in claim 28. The Examiner does not contend that these additional limitations are disclosed in any of Ginter, Cocotis, Cooper, Mott, Challener or Unicate, since none of these references were applied against claim 28: claim 28 was rejected only over the XTEC reference. Claim 28 is amended hereby to recite that the encryption key is generated from characters stored in the "authentication data" instead of in the "authentication table." Neither claim 28 – nor any of the other claims, as amended, pending in this application – relate to a system in which a first party to a transaction provides a second party to that transaction (such as a server) with a decrypt key, or with authentication data.

Rejections under 35 USC § 102

Claim 28

The Examiner's rejection of claim 28 as anticipated by XTEC, to the extent that it might be applied against claim 28 as presently amended, is respectfully traversed. XTEC nowhere discloses gathering session specific data, and hashing the session specific data to obtain reference numbers referring to positions in authentication data, and then generating the encryption key from the characters stored in the authentication data. Instead, at page 6, lines 6-8, XTEC explains that location information is combined with the data contained in selected locations to construct data for use in generating cryptoprocessing keys. Accordingly, claim 28 is clearly neither anticipated by, nor obvious, in view of the XTEC reference.

The cryptoprocessing key structure referred to in the XTEC reference requires elaborate key management systems and operations by an issuer of public and private key pairs. It also requires the distribution of the private keys in a secure manner. The private key is applied *in its entirety* to encrypt data, and the public key is also applied *in its entirety* to decrypt data. The digital signatures are *verified* by the recipient. The parties must have systems and applications at both ends of the system so that the recipient can retrieve the public key to perform the decrypt function. The private key/public key system disclosed in the prior art does not create or derive transaction specific session keys, *i.e.*, it does not use only a part of either the public key or the private key. In a cryptoprocessing key system disclosed in the reference, it is impossible to encrypt data with only a part of a private key, and to decrypt the data with an entire public key.

Private and public keys are distributed only once, and therefore are static and non-session specific. Moreover, the reference does not disclose any relationship between session specific data and any key corresponding to (dynamic) session keys.

Claim 28 is also not obvious in view of the combination of XTEC with Cocotis and/or Ginter. Like XTEC, neither of those references discloses gathering session specific data, and hashing the session specific data to obtain reference numbers referring to positions in authentication data, and then generating the encryption key from the characters stored in the authentication data. Instead, Ginter discloses an SPU that is enclosed within and protected by a "tamper resistant security barrier," that separates the secure environment from the rest of the world; and Cocotis discloses a public key/private key encryption system. (Ginter, paragraphs [0444]-[0448]; Cocotis, paragraph [0017]-[0018].) The other references cited by the Examiner also do not supply the missing elements recited above. Instead, Cooper discloses a system that uses a Certificate Authority such as Verisign, and requires two hashing operations involving the private keys of the B2C partner and the end user (Cooper, blocks 440 and 450 in Figure 4 and column 29, lines 17-26); Mott relates to targeting a digital information playback device by embedding a device or group ID in the device, so as to limit the playback to a specified player or group of players (Mott, col. 2, lines 9-19; col. 5, lines 15-31; col. 7, lines 24-42; and col. 12, lines 19-59); Mott also discloses a verification sequence in which each one of two systems requests verification from the other system and provides authentication in the form of pre-defined sets of bit streams in response to the request (Mott, col. 11, line 50 to col. 12, line 11); Challener relates to securely updating a root of trust measurement (RTM) function in a personal

computer to ensure that the personal computer is updated in a manner that ensures that the update is authentic (Challener, paragraphs [0006]-[0007]; and Unicate explicitly disavows any use of cryptography, and instead registers profiles comprising a party identifier and authentication data (Unicate, page 1 lines 31-35 and page 5, lines 15-28).

Claims 1 and 29

Claims 1 and 29 have been amended to recite the limitations discussed above with respect to claim 28. Accordingly, claims 1 and 29, as well as claim 1's dependent claims, are patentable for the reasons provided above with respect to claim 28.

Claims 1 and 29, as amended, are also patentable because they are not anticipated by or obvious in view of Ginter, Cocotis or XTEC.

Ginter discloses an SPU that processes information in a secure processing environment, and is enclosed within a tamper resistant security barrier. (Ginter, paragraphs [0444]-[0448].) An SPE reads information from the secure database records in encrypted form, and decrypts it based upon access keys stored within the protected memory of the SPU. (Ginter, paragraph [1302].) The SPE sends blocks of information to the encrypt/decrypt engine along with the key needed to decrypt the information. (Id.) In transferring electronic currency or credit, Ginter discloses using identification for a digital signature and using a transaction certificate so that the transaction may not be repudiated. (Ginter, paragraph [1813].) The digital signatures may comprise conventional digital signatures using public keys. (Ginter, paragraph [1913].) Claims 1 and 29 are not anticipated by, and are patentable, over Ginter because none of these steps anticipates or in any way suggests the method recited in claims 1 and 29, as amended, in which

the digital signature is generated from the authentication data by gathering session specific data, hashing that session specific data to obtain reference numbers referring to positions in the authentication data, and generating the digital signature from characters stored in the authentication data at those positions.

Cocotis discloses the client accessing an embedded public key corresponding to the private key used by the server to validate server digital signatures. (Cocotis, paragraph [0043], [0061], [0067].) Unlike the disclosure in Cocotis, claims 1 and 29 do not recite a method in which one party to the transaction provides the other party with a public key, or recites digital signing by the second transaction party which is then verified by the first transaction party. Accordingly, claims 1 and 29, and their dependent claims, are not anticipated by, and are patentable, over Cocotis, because Cocotis does not disclose or suggest the method recited in claims 1 and 29, as amended, in which the digital signature is generated from the authentication data by gathering session specific data, hashing that session specific data to obtain reference numbers referring to positions in the authentication data, and generating the digital signature from characters stored in the authentication data at those positions.

The Ginter and Cocotis references disclose asymmetric private key/public key cryptographic structure. As pointed out above, the private key/public key structure requires elaborate key management systems and operations by the issuer of the public and private key pairs. It also requires the distribution of the private keys in a secure manner. The private key is applied *in its entirety* to generate a digital signature or to encrypt data, and the public key is also applied *in its entirety* to verify a digital signature or to decrypt data. The digital signatures are

verified by the recipient. The parties must have systems and applications at both ends of the system so that the recipient can retrieve the public key to perform the decrypt function. The private key/public key system disclosed in the prior art does not create or derive transaction specific session keys, *i.e.*, it does not use only a part of either the public key or the private key. In a private key/public key system disclosed in the prior art, it is impossible to generate a digital signature or to encrypt data with only a *part* of a private key, and to validate the digital signature or decrypt the data with an (entire) public key. Private and public keys are distributed only once, and therefore are *static* and *non-session specific*. Moreover, the prior art does not disclose any relationship between session specific data and any key corresponding to (dynamic) session keys.

As pointed out above, XTEC discloses using location information that is combined with the data contained in selected locations to construct data to generate cryptoprocessing keys. XTEC nowhere discloses gathering session specific data, and hashing the session specific data to obtain reference numbers referring to positions in authentication data, and then generating the encryption key from the characters stored in the authentication data. Accordingly, claim 1 and its dependent claims, as well as claim 29, are patentable because they are not anticipated by or suggested by the XTEC reference.

As also pointed out above, the other prior art of record and relied upon by the Examiner in this application (*i.e.*, Cooper, Mott, Challener and Unicate) do not supply the limitations of claim 28 that are not disclosed in the XTEC reference. Accordingly, claims 1 and 29 are patentable over the prior art of record in this application.

Claims 2-5, 7-8 and 10-27

These claims are patentable because they depend upon claim 1, which is patentable as discussed above. Furthermore, claims 5 and 7 are further distinguished from the prior art relied upon by the Examiner because claim 5 requires that the authentication data are stored by the second transaction party, which stores that data together with data identifying the first transaction party, and claim 7 further recites that the second transaction party verify the digital signature provided by the first party using the stored authentication data. This is in contrast to the public key/private key system, in which the private key may only reside with the party to whom the private key has been issued, *i.e.*, the private keys may not be stored by the second transaction party. Also, claim 8, as amended, is further distinguished form the prior art of record because claim 8 requires the first transaction party to use a private key that is provided by a trusted third party, and is not known by the second transaction party.

Claims 31 and 32

The claims both include the gathering session specific data, and hashing the session specific data to obtain reference numbers referring to positions in authentication data, and then generating the encryption key from the characters stored in the authentication data. These limitations are discussed above with respect to claims 1, 28 and 29, and therefore claims 31 and 32 are patentable for the reasons provided above with respect to those claims.

Conclusion

In view of the foregoing all of the claims in this case are believed to be in condition for allowance. Should the Examiner have any questions or determine that any further action is

desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone applicants' undersigned representative at the number listed below.

PAUL, HASTINGS, JANOFSKY & WALKER LLP
875 15th Street, N.W.
Washington, D.C. 20005
Tel: 202-551-1700

Respectfully submitted,

Date: May 28, 2010

By: 
Aslan Baghdadi
Registration No. 34,542

AB/hjm

Customer No. 36183